IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN, Plaintiff, V. UNITED STATES, Defendant.	1:13-cv-307-EGB Senior Judge Eric G. Bruggink September 7, 2021

PLAINTIFF'S RESPONSE TO DEFENDANT'S MOTION TO STRIKE AND PLAINTIFF'S MOTION FOR SUMMARY JUDGEMENT

Patent Claims 4, 5, & 6 of the '287 patent in the PIC Charts demonstrates how Apple and Samsung; Apple and TSMC; Qualcomm and LG; and, Qualcomm and Samsung are potentially liable under the provisions of *joint direct infringement*. *Akamai Techs*., 629 F.3d at 1319-21 (holding there must be a contractual or agency relationship between the parties for a finding of joint infringement) **(Qualcomm—Exhibits A & B)**

The Cell-All program is funded and managed by HSARPA, whose mission is to facilitate the rapid development and deployment of new security technologies, mainly through partnerships and contracts with the private sector (U.S. Depart. of Homeland Security, 2011a).

Specifically, "the purpose of infringement contentions is to provide notice of the plaintiff's theories of infringement early in the case because, in practice, it is difficult to obtain such information through traditional discovery means, such as interrogatories." *Sloan Valve Co. v. Zurn Indus.*, 2012 U.S. Dist. LEXIS 176554, *6-7 (N.D. Ill. Dec. 13, 2012) (St. Eve, J.).

"Given that the Infringement Contentions are exchanged prior to discovery, this chart will likely be based solely on publicly available information" *2018 AIPLA Local Patent Rules.*

Plaintiff need not identify every piece of evidence on which it will ultimately rely to show infringement in its infringement contentions. *See Innovation IP Ventures, LLC Patent Litig.*, 956 F. Supp. 2d 925, 940-41 (N.D. Ill. 2013) (Holderman, C.J.).

PRECEDENCE FOR ENFORCING PATENT LOCAL RULES

Preliminary Infringement Contentions

"[Plaintiff] has the burden of proof with respect to infringement and had to provide notice of its legal theories in view of the information revealed through discovery. . . There is no new information that requires an amendment. The only thing that has changed is the Defendants' legal theory. In other words, ... all that has changed is how the Defendants' view the facts in the context of [Plaintiff's] allegations. This does not establish good cause." *Northgate Techs., Inc. v. Stryker Corp.*, 1-12-cv07032 (N.D. Ill. Dec. 16, 2013) (Kendall, J.).

"Nor could [Plaintiff] reasonably rely on the positions the Defendants' took in their initial non-infringement contentions as evidence of infringement. The Local Patent Rules make clear that initial disclosures are inadmissible as evidence on the merits. LPR 1.6. Their purpose is to enable the parties to identify likely issues in the case and to enable them to focus and narrow their discovery requests. They are a vehicle through which the party that bears the burden of proof on an issue provides notice of its legal theories to the other party. . . In turn, the party that does not have the burden of proof on an issue provides its legal theories with respect to that issue in its responsive contentions." *Northgate Techs., Inc. v. Stryker Corp.*, 1-12-cv-07032 (N.D. Ill. Dec. 16, 2013) (Kendall, J.).

"Given that the Infringement Contentions are exchanged prior to discovery, this chart will likely be based solely on publicly available information. Prior to the service of Infringement Contentions, a party asserting infringement need only take reasonable steps as required by Rule of 11 of the Federal Rules of Civil Procedure to assert infringement in the Complaint. For example, prior to the service of Preliminary Infringement Contentions, a party asserting infringement need not go to the expense of reverse engineering every publicly available product because of the ready availability of information during discovery. If additional information is obtained during discovery, the Infringement Contentions should be diligently updated." *2018 AIPLA Model Local Patent Rules*

"While there is some uncertainty as to the requisite level of detail required to satisfy the requirements of local rules governing initial infringement contentions, all courts agree that the contentions "must be sufficient to provide reasonable notice to the defendant why the plaintiff believes it has a 'reasonable chance of proving infringement.'" *Shared Memory Graphics LLC v.*

Apple, Inc., 812 F. Supp. 2d 1022, 1025 (N.D. Cal. 2010) (quoting *View Eng'g, Inc. v. Robotic Vision Sys., Inc.*, 208 F.3d 981, 986 (Fed. Cir. 2000)).

"It is not a verbatim recital of the text of the claim. (*Id*.) Rather, it discloses some of its factual bases and, albeit without precision, provides reasonable notice of why… believes that it will prevail on this infringement claim." *Shared Memory Graphics*, 812 F. Supp. 2d at 1025.

"Those contentions that Keeler has merely paraphrased are simpler ones, usually to the point that Keeler would be hard-pressed to phrase its contentions otherwise. Therefore, the contentions are not vague or conclusory in a way that prevents them from serving to give notice to Heron Point. Id. While the court is aware of the fact that Keeler poses its contentions without the benefit of having examined the accused product, such is the position of all plaintiffs at this stage in the litigation. The infringement contentions now at issue are merely preliminary. After Keeler has been given an opportunity for discovery, it may seek to amend its contentions, if necessary, before they become final following the construction hearing." *See* L.P.R. 3.10.

"Specifically, the purpose of infringement contentions is to provide notice of the plaintiff's theories of infringement early in the case because, in practice, it is difficult to obtain such information through traditional discovery means, such as interrogatories." *Sloan Valve Co. v. Zurn Indus.*, 2012 U.S. Dist. LEXIS 176554, *6-7 (N.D. Ill. Dec. 13, 2012) (St. Eve, J.).

"[A] party need not identify every piece of evidence on which it will ultimately rely to show infringement in its infringement contentions. Instead, it need only identify 'where each element of each asserted claim is found within each Accused Instrumentality.' [Plaintiff's] infringement contentions might successfully perform this task with respect to non-standard essential claims without citing any sources other than the 802.11 standard. Accordingly, [Plaintiff's] failure to cite to anything beyond portions of the 802.11 standard in its infringement contentions with respect to a particular patent claim does not limit [Plaintiff] to using only those portions of the standard to prove its case." *In re Innovation IP Ventures, LLC Patent Litig.*, 956 F. Supp. 2d 925, 940-41 (N.D. Ill. 2013) (Holderman, C.J.).

"Defendant is correct that the stated purpose of the IICs [Initial Infringement Contentions] 'is to identify the likely issues in the case, to enable the parties to focus and narrow their discovery requests,' but that is not the same as limiting the scope of discovery to only the products listed in the IICs, or requiring the Final Infringement Contentions to be identical to the IICs. . . Case law from various circuits clearly states that there is no bright-line rule limiting

discovery to only those products specifically accused in a party's infringement contentions. Rather, the rule is that discovery concerning products not explicitly listed in the infringement contentions is appropriate when: (1) the infringement contentions give notice of a specific theory of infringement; and (2) the products for which a plaintiff seeks discovery operate in a manner reasonably similar to that theory. . . Thus, the issue for the Court is whether the products sought in [Plaintiff's] discovery requests operate in a manner reasonably similar to the theory of infringement listed in the IICs." *Micro Enhanced Tech., Inc. v. Videx, Inc.*, 1-11-cv-05506 (June 28, 2013) (Valdez, M.J.).

"Because the purpose of infringement contentions is to provide notice of the plaintiff's theories of infringement early in the case, and [Plaintiff] is not, by its own concession, seeking to change its theory, this proposed amendment to its contentions is unnecessary." *Sloan Valve Co. v. Zurn Indus.*, 2013 U.S. Dist. LEXIS 22739, *9 (N.D. Ill. Feb. 20, 2013) (St. Eve, J.).

Final Infringement Contentions

"[T]he local patent rules require the plaintiff to file its final infringement contentions after the close of fact discovery, but before claim construction and expert discovery…" *Sloan Valve Co. v. Zurn Indus.*, 2014 U.S. Dist. LEXIS 1208, 11-12 (N.D. Ill. Jan. 7, 2014) (St. Eve, J.)

"A party claiming patent infringement must serve on all parties "Final Infringement Contentions" containing the information required by LPR 2.2 (a)–(h) within twenty-one (21) weeks after the due date for service of Initial Infringement Contentions. Each party asserting invalidity or unenforceability of a patent claim shall serve on all other parties, no later than the same time that the Final Infringement Contentions are due…"

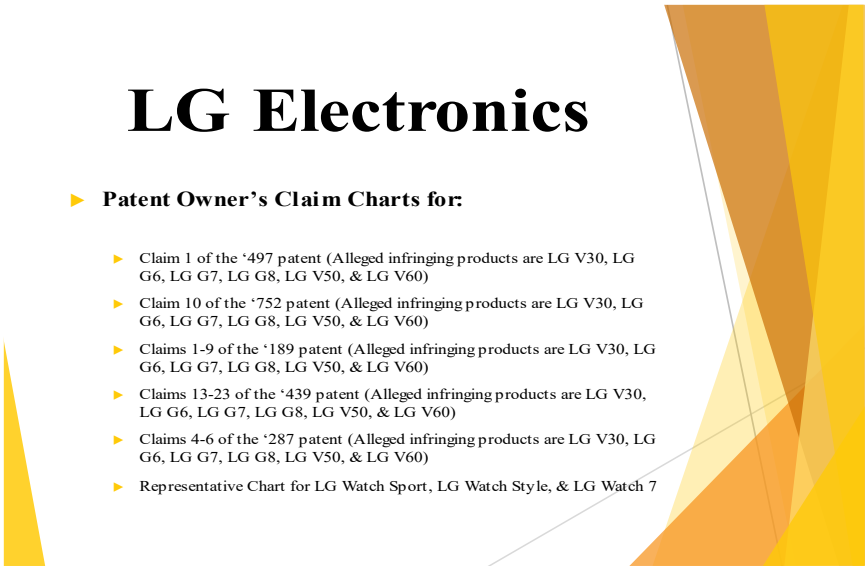
"[Defendant contends that Plaintiff's] Final Infringement Contentions do not provide any evidence of actual usage of the accused products. [Plaintiff] asserts that the Local Patent Rules do not require it to point to 'specific, actual use of the product'… Nor do the rules require the 'reasonably capable' analysis that [Defendant] contends [Plaintiff] must demonstrate in its Final Infringement Contentions. This Court agrees that the Local Patent Rules do not require the Final Infringement Contentions to provide evidence of actual usage of the accused products." *Trading Techs. Int'l, Inc. v. CQG, Inc.*, 2014 WL 4477932, *4 (N.D. Ill. Sept. 10, 2014) (Coleman, J.).

"Plaintiffs' Final Infringement Contentions included a detailed description of the Accused Structure and a photograph with red marks drawing attention to the toggle, making

clear that the toggle played an important role in the infringement claim. The arguments in Plaintiffs' subsequent expert reports and motions are consistent with this suggestion. The Final Infringement Contentions therefore gave Defendants fair notice of Plaintiffs' theory of infringement, satisfying the purpose of the local patent rules. The absence of the particular words 'pivot lever' in the Contentions is to be expected; the Court did not use those words in its claim construction opinion until over one year later. Requiring an amendment in these circumstances would only prolong the litigation, increasing the costs to both parties and needlessly wasting judicial resources. Accordingly, the Court finds that Plaintiffs' argument is not procedurally barred." *The Black & Decker Corp. v. Positec USA Inc.*, 11-cv-5426 (N.D. Ill. Mar. 31, 2015) (Dow, J.)

EXAMPLE OF HOW PLAINTIFF HAS COMPLIED WITH RULE 4 OF THE PATENT LOCAL RULES

(a) the claim in each product, process, or method of each patent at issue that is allegedly infringed by each opposing party;



(b) for each asserted claim, each product, process, or method that allegedly infringes the identified claim. This identification must include the name and model number, if known, of the accused product, process, or method;

LG's
New and Improved Cell Phones

LG V30

LG G6

LG's
Watch Sport

Radiation and Chemical Detection

Medical Chem/Bio Detection

LG's
New and Improved Cell Phones

LG G7

LG G8

LG's
Watch Style

Radiation and Chemical Detection

Medical Chem/Bio Detection

LG's
New and Improved Cell Phones

LG V50

LG V60

LG's
Watch 7

Radiation and Chemical Detection

Medical Chem/Bio Detection

(c) a chart identifying where each element of each asserted claim is found within each accused product, process, or method, including the name and model number, if known; include, if governed by pre-AIA 35 U.S.C. § 112(6) or post-AIA 35 U.S.C. § 112(f). 4(c) is described in greater detail throughout this document.

> *"Given that the Infringement Contentions are exchanged prior to discovery, this chart will likely be based solely on publicly available information. Prior to the service of Infringement Contentions, a party asserting infringement need only take reasonable steps as required by Rule of 11 of the Federal Rules of Civil Procedure to assert infringement in the Complaint. For example, prior to the service of Preliminary Infringement Contentions, a party asserting infringement need not go to the expense of reverse engineering every publicly available product because of the ready availability of information during discovery. If additional information is obtained during discovery, the Infringement Contentions should be diligently updated." 2018 AIPLA Model Local Patent Rules*

(d) whether each element of each identified claim is alleged to be literally present or present under the doctrine of equivalents in the accused product, process, or method; **(Charts for Apple, Dkt. No. ???; Samsung, Dkt. No. ???; and LG, Dkt. No. ???; were filed on 08/18/21)**

Patent #: 7,385,497; Independent Claim 1	**LG Electronics LG V30 & LG G6 Series and LG Watch Sport Series**
A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:	**Plaintiff believes the Defendant and third-party contractor; LG Electronics' is literally infringing Plaintiff's claim limitation for Plaintiff's CMDC device(s).** **LG Electronics LG V30 & LG G6 Series** are believed to be communicating, monitoring, detecting, and controlling (CMDC) devices of at least one of the *new and improved* products grouped together by common features in the product groupings category of design similarity (i.e., computer terminal, personal computer (PC), laptop, desktop, notebook, handheld, cell phone, PDA or smart phone); that comprises, are interconnected to, or integrated with, at least a Central Processing Unit (CPU), that is vital for processing instructions; an Operating System (OS); mobile apps developed for the CMDC devices operating system (OS) such as Android, Apple® iOS®, BlackBerry®, or Windows® Mobile; wireless protocol of Cellular, Bluetooth, Wi-Fi, etc., and CBRNE-H sensors that are placed in, on, upon, or adjacent the *new and improved* CMDC devices; interconnected to the CMDC devices for communication therebetween. **IPR Final Written Decision**. "In the Decision to Institute, we construed certain claim terms. Those constructions are reproduced… "communication device" is construed to mean "monitoring equipment"; and, "built in, embedded" is construed to include ""something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device". Patent Owner argues that "[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals." "As Patent Owner explains, the added language is broad enough to

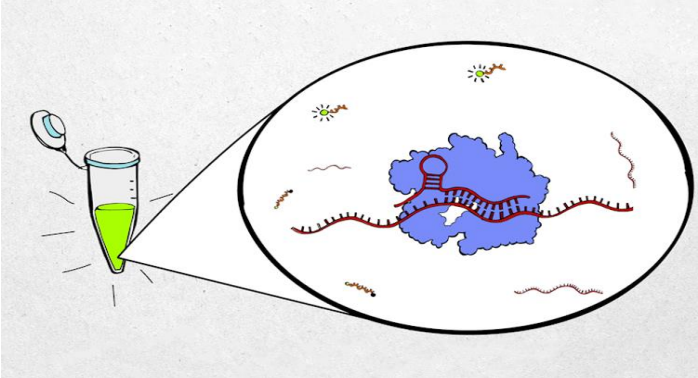
include the removed items, and is intended to reflect the entire genus of "monitoring equipment" and "communications devices" that "are capable of communication and capable of receiving signals." Mot. to Amend 4, 5. Thus, the claim has been broadened to not only include the listed species that have been removed, but anything falling within the claimed genus." UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Petitioner, v. LARRY GOLDEN, Patent Owner. Case IPR2014-00714. Entered: October 1, 2015

The Department of Homeland Security's Cell-All project. "Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones…" "During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their current phones before integrated sensors are fully operational and readily available." Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. Torin Monahan & Jennifer T. Mokos: A Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA; and, a Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

DHS Cell-All Chemical Sensors: Qualcomm first introduced a "built-in, embedded" chemical sensor for the smartphone (picture below). Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded ''sleeve'' for phones (picture below); that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)." **(Qualcomm—Exhibits A & B)**

CMDC Device Camera Sensor for Biological Detection: "In the diagnostic test (below), a patient sample is mixed with CRISPR Cas13 proteins (purple) and molecular probes (green) which fluoresce, or light up, when cut. When coronavirus RNA is present in the sample, it prompts the CRISPR proteins to snip the molecular probes, causing the whole sample to emit light. This fluorescence can be detected with

a cell phone camera." (*Image courtesy Science at Cal*). The COVID-19 virus is perceived as a biological weapon of mass destruction (BWMD).



CMDC Device Geiger Counter for Radiological Detection: Below is a picture of a "Smart Geiger Counter Nuclear Radiation Dosimeter "X-Ray" and "Gamma" Detector Smartphone Android iOS with App". Real-time display of measurement results. Ultra-low power consumption. World smallest Geiger Counter (30mm). Compatible with Android and iOS.

Smartwatch: To use a smartwatch as a stand-alone detection device, you need a smartphone. On the smartphone, the user installs the app that comes with the smartwatch stand-alone detection device, such as Android Wear (Wear OS—operating system) or Watch from Apple (i.e., watch OS/7—operating system). By opening the accompanying app on the smartphone and turning on Bluetooth, the user can synchronize the smartwatch to function as a stand-alone detection device with the smartphone.

Central Processing Unit (CPU): The Central Processing Unit (CPU) is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that is vital and essential processes and executes program instructions.

Patent Specifications: "In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs,

	notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring… a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween… or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted… The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174… the integration of portable electronic communication or telecommunication devices such as a cell phone 187a and/or a laptop computer 187b with the monitoring equipment 138 located at a predesignated monitoring site 188…" ********** **Plaintiff believes the Defendant and third-party contractor; LG Electronics' is infringing Plaintiff's claim limitation under the "doctrine of equivalents" for Plaintiff's "lock disabling system", that is interconnected to, or integrated with, Plaintiff's CMDC device(s).** **Patent Specifications**: "FIG. 1 is a perspective view of the… an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler… FIG. 14 is a representative schematic view of the… lock disabling system of the present invention illustrating interconnection of the… fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public… The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40… for receiving transmissions therefrom after detection… has occurred so that the lock… can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56… a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock… The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety… and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108" **Example:** Security feature: After several unsuccessful log-in attempts using a passcode or fingerprint, an Android device automatically locks itself up. If unable to log in after the security layers, the only option is to have the device unlocked. The wrong pin will launch to Google Account Login. On Android Phone, multiple attempts (usually five attempts) with an unknown or a wrong pin will go either into a 30 seconds delay before further attempts are allowed or the phone will allow entry using your Google account password to unlock the phone. You can have your irises and multiple fingerprints registered along with a backup PIN, pattern or password. "Lock Network & Security" feature as my security net if my phone is stolen. The "Lock Network & Security" feature is supposed to prevent anyone else from turning OFF your phone and your wifi/data when your phone is locked, for purposes such guaranteeing that you will still be able to track or remotely control your phone when it is lost or stolen.

a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);	**Plaintiff believes the Defendant and third-party contractor; LG Electronics' is literally infringing Plaintiff's claim limitation** **Central Processing Unit (CPU)**: The Central Processing Unit (CPU) of the alleged infringing devices are the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e., communication devices, monitoring device; monitoring equipment). The components for a processor are condensed to fit in the smartphone, and exist as a mobile application processor, or a System-on-a-Chip (SoC), that includes the CPU. Mobile application processors are found in smartphones, smartwatches, and tablets.

(e) for each patent that claims priority to an earlier application, the priority date to which each asserted claim allegedly is entitled and whether the patentee is relying on the filing date or an earlier conception date as the priority date. **(Dkt. No. ???; filed 08/23/21)**

Each asserted independent claim of the '752, '189, '439, & '287 patents (i.e., 24 claims) are allegedly entitled to the filing date of the '497 patent.	Filing date of the '497 patent is ***04/05/2006***

Each asserted independent claim of the '497, '752, '189, '439, & '287 patents (i.e., 25 claims) are allegedly entitled to the filing date of the Plaintiff's Disclosure Document filed with USPTO. Doc. No. 565732	Disclosure Document filed on ***11/26/2004***

Each asserted independent claim of the '497, '752, '189, '439, & '287 patents (i.e., 25 claims) are allegedly entitled to the "conception of the technical rational"; inventions Plaintiff alleged are major components to the completion of Plaintiff's three economic stimulus packages submitted to the Government. The Affidavit submitted under 37 CFR §1.131 and §1.132 into record of the '752 patent (IFW) on 07/21/2010, establishes a priority date of Dec. 16, 2002 to overcome 102 and 103 objections.[1] ***A true copy of the documents' evidencing conception is attached at Dkt No.???x; filed 08/23/21***	Earlier conception filed with the Honorable Congressman Elijah E. Cummings: ***12/16/2002***

[1] PATENT RULES OF THE UNITED STATES COURT OF FEDERAL CLAIMS: Rule 5. Document Production Accompanying Preliminary Disclosure (b) all documents that evidence the conception and first reduction to practice of each claimed invention that was created on or before the date of application for each patent at issue or the priority date identified in PRCFC 4(e). Plaintiff's Invalidity Contentions is discussed later in this document.

PLAINTIFF'S 'CPUs' ARE THE DOMINANT COMPONENTS IN PLAINTIFF'S CMDC DEVICES

Without Plaintiff's CPUs in His CMDC Devices, the Devices Would Not Be Able to Function, and Would Therefore Lack Utility

In Plaintiff's CMDC (i.e., new and improved cell phones; smartphones) devices, the CPU is responsible for the execution of most of the functions of the mobile devices. These functions include running apps and the operating system, as well as relaying input instructions from the user to the rest of the device (smartphonedomain.com., 2021).

Your smartphone processor, also known as chipset, is a component that controls everything going on in your smartphone and ensures it functions correctly. You can compare it to the brain of the human body. Every action you perform on your smartphone goes straight to the processor. https://www.coolblue.nl/en/advice/smartphone-processors.html

"Unlike simpler mobile phones of the past, today's smartphones all have processors or CPUs. ***A smartphone CPU (central processing unit) is the brains of the entire device. Without one, no smartphone would be able to function***" (smartphonedomain.com., 2021).

A CPU, at its most basic level, consists of five parts:

- *Arithmetic and logic unit (ALU)*: The ALU is responsible for performing calculations on data. An uncomplicated CPU might contain just one ALU that can perform only addition, subtraction, and basic logic. The more sophisticated CPUs may contain several ALUs that are capable of advanced floating-point operations (McGrath, 2014).
- *Control unit (CU)*: The CU controls the movement of instructions in and out of the processor, as well as the operation of the ALU (McGrath, 2014).
- *Register array*: A register array consists of small units of internal memory used for quick storage and retrieval of data and instructions. All processors contain at least one program counter, an instruction register, an accumulator, a memory address register, and a stack pointer register (McGrath, 2014).
- *System bus*: The system bus comprises a data bus, an address bus, and a control bus and is used to transfer data between the processor, memory, and peripherals. The address bus carries the address of a specified location. The data bus carries information between the CPU

and memory, or between the CPU and I/O devices. The control bus carries commands from the CPU and returns status signals from the devices (McGrath, 2014).

- *Memory*: Although not actually part of the CPU, memory is an essential part of CPU operation as it stores data and the program being executed (McGrath, 2014).

The instruction set architecture (ISA) describes a list of instructions that a processor (CPU) understands. Different processors have different instruction sets, which are optimized for the features of that processor. Each instruction consists of a short code, called an opcode, describing the operation the CPU is expected to perform

McGrath, M. J., (2014, Jan. 4). Key Sensor Technology Components: Hardware and Software Overview. Retrieved from: https://link.springer.com/chapter/10.1007/978-1-4302-6014-1_3

smartphonedomain.com (2021, Jan. 25). Does A Phone Have A CPU? Does A Smartphone Have A CPU? Retrieved from: https://smartphonedomain.com/does-a-phone-have-a-cpu/

The list below contains the most common components that you will find inside a smartphone system-on-a-chip.

- *Central Processing Unit (CPU)* — The "brains" of the SoC. Runs most of the code for the Android OS and most of your apps.
- *Graphics Processing Unit (GPU)* — Handles graphics-related tasks, such as visualizing an app's user interface and 2D/3D gaming.
- *Image Processing Unit (ISP)* — Converts data from the phone's camera into image and video files.
- *Digital Signal Processor (DSP)* — Handles more mathematically intensive functions than a CPU. Includes decompressing music files and analyzing gyroscope sensor data.
- *Neural Processing Unit (NPU)* — Used in high-end smartphones to accelerate machine learning (AI) tasks. These include voice recognition and camera object segmentation.
- *Video encoder/decoder* — Handles the power-efficient conversion of video files and formats.
- *Modems* — Converts wireless signals into data your phone understands. Components include 4G LTE, 5G, WiFi, and Bluetooth modems.

CPUs inside smartphone SoCs come in an assortment of flavors, all of which are based on the Arm CPU architecture. The latest CPU cores from Arm are the big Cortex-X2 and Cortex-A710, along with the little Cortex-A510.

Written Description of Plaintiff's 'CPUs' in the Specifications of the Asserted Patents ('497, '752, '189, '439, & '287)

"Internet and GPS connections and a ***cpu*** interconnected with the Internet and GPS connections… [e]ach detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the ***cpu***… the detection of the particular agent or compound can be conveyed from the detectors to the detector case ***cpu***… [a] ***cpu*** 40 is mounted within the detector case 12 and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment… [t]he detectors 46 are interconnected to the ***cpu*** 40 of the detection system 10 by conventional connections that can be wire or wireless for transmitting the appropriate signals to the ***cpu*** 40 upon detection of the particular agent or compound… [e]ach detector 46 includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the ***cpu*** 40 of the detector case 12… FIGS. 4 and 5 and connected by wire 58 to the ***cpu*** 40 of the detector case 12… [t]he fingerprint biometric lock with disabler 62 is interconnected to the ***cpu*** 40… resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the ***cpu*** 40, then the individual can reset the fingerprint biometric lock with disabler… he lock disabler 56 would be activated upon detection of the harmful agent or compound and receipt of a signal from the ***cpu*** 40… a representative schematic 74 for describing the signal transmission process from the detector 46 to the ***cpu*** 40… detection of the specific agent will trigger the sound alarm 80 and the light alarm 82, and instant transmittal of a signal to the ***cpu*** 40… [t]he readings 84 can be stored by the ***cpu*** 40 for verification and future review and evaluation… the system 10--the ***cpu*** 40--will transmit a lock/disable lock signal 94 to the automatic/mechanical lock disabler 56 to lock or disable the lock on the product… [u]pon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the ***cpu*** 40 would then transmit a signal to the fingerprint biometric lock with

disabler 62 to lock or disable the lock on the product… [t]he ***cpu*** 40 would transmit a lock/disable signal 120…"

DHS "*CELL-ALL*" THIRD-PARTY CONTRACTOR – QUALCOMM, INC.

Qualcomm is undoubtedly the most widely known company because its Snapdragon smartphone processor can be found in quite a number of today's smartphones. Other companies include Apple (A-series), Samsung (Exynos), and others that are featured below. Remarkably, although Apple designs their own processors, some of the Apple iPhone processors have been made by Samsung. Smartphone CPU manufacturers usually have a series of processors that perform differently **(Qualcomm—Exhibits A & B)**.

(smartphonedomain.com., 2021).

Qualcomm is the largest provider of smartphone SoCs, shipping chips for the majority of flagship, mid-tier, and even low-end smartphone releases each ear. Qualcomm's SoCs fall under the Snapdragon branding. Premium chips boasting the company's best technology come under the Snapdragon 800 series banner, such as the latest Snapdragon 888. The Snapdragon 765 is a mid-range chip that sports 5G connectivity. https://www.androidauthority.com/what-is-an-soc-smartphone-chipsets-explained-1051600/

Patent Claims 4, 5, & 6 of the '287 patent in the PIC Charts demonstrates how Apple and Samsung; Apple and TSMC; Qualcomm and LG; and, Qualcomm and Samsung are potentially liable under the provisions of "joint direct infringement. *Akamai Techs*., 629 F.3d at 1319-21 (holding there must be a contractual or agency relationship between the parties for a finding of joint infringement…)

Example of Qualcomm's SoC / CPUs: (Qualcomm—Exhibits A & B)

Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
Qualcomm's DHS Government Contract **Government Industry**	HSARPA conducted a national search for ideas that was intended to leverage existing technological expertise in the public and private sectors, which led to the creation of six workable first generation prototypes, including a ''form factor phone'' developed by Qualcomm and a chemical nano-sensor device developed by NASA (U.S. Department of Homeland Security, 2011a). Research contracts were awarded by DHS through HSARPA and the Small Business Innovation Research Portfolio, with some of the primary recipients being Qualcomm, Synkera Technologies, and NASA (U.S. Department of Homeland Security, 2011b). In addition, DHS S&T secured Cooperative Research and Development Agreements with four primary cell phone manufacturers—Qualcomm, LG, Apple, and Samsung—with the objective of accelerating the ''commercialization of technology developed for government purposes'' (U.S. DHS, 2010).
Qualcomm® Snapdragon™ (SoC / Central Processing Unit (CPU)) **Government Industry: Industry for Processors**	Snapdragon is a suite of system on a chip (SoC) semiconductor products designed and marketed by Qualcomm for mobile devices. The Snapdragon system on chip (SoC) was announced in November 2006. The Snapdragon central processing unit (CPU) uses a single SoC that may include multiple CPU cores, a wireless modem, and other software and hardware to support a smartphone's global positioning system (GPS), camera, gesture recognition and video. We are helping protect our U.S. government partners' communication with a combination of authentication and identification methods. Our best-in-class commercial sensors help ensure accurate authentication and trusted access for users and devices. From biometrics that reduce or eliminate the need for passcodes, to advanced hardware that shields your data, the Qualcomm® Snapdragon™ mobile security platform is designed to guard and protect precious data with vault-like security. Qualcomm Snapdragon is a product of Qualcomm Technologies, Inc., and/or its subsidiaries. https://www.qualcomm.com/products/government/authentication-identity
Qualcomm Government Technologies **Government Industry**	Qualcomm Government Technologies leverages Qualcomm's wireless expertise, innovative technologies and vast industry reach to provide capabilities and services that enable our government customers to realize significant technology gains and excellence in mission performance. Qualcomm Incorporated (www.qualcomm.com) is a leader in developing and delivering innovative digital wireless communications products, services, and other advanced technologies. https://www.qualcomm.com/news/releases/2008/05/29/qualcomm-government-technologies-extends-software-security-cryptographic

Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
Qualcomm's DHS Government Contract **Government Industry**	FAIRFAX, Va.--(BUSINESS WIRE)--Kryptowire, the mobile application security and privacy testing platform of choice for U.S. government agencies, is delighted to announce that the Qualcomm Technologies, Inc., has been awarded $1.8M by the Department of Homeland Security Science and Technology Directorate (DHS S&T) to demonstrate Qualcomm Technologies' hardware-anchored Mission-Critical-Grade Security Layer (MCGSL) that leverages the Snapdragon Mobile Security Platform and extends its foundational commercial capabilities to Kryptowire's military-grade mobile application security testing platform to address threats on commercial mobile devices. *
NFC **Wireless Networking Technology Industry**	NFC chips might also be widely used in the Internet of Things. Qualcomm recently announced that it will include NXP's near-field communication (NFC) solution in the Snapdragon processor platform that powers mobile devices (e.g., smartphones), wearables (e.g., smartwatches), and automobiles. *
SmartWatch Qualcomm® Snapdragon Wear™ 4100+ platform **Wireless Networking Technology Industry**	The Qualcomm® Snapdragon Wear™ 4100+ platform, comprised of a powerful applications processor and ultralow power co-processor, is designed to deliver super-fast performance, and connectivity. Like other computers, a smartwatch may collect information from internal or external sensors and it may control, or retrieve data from, other instruments or computers. It may support wireless technologies such as Bluetooth, Wi-Fi, and GPS. The Qualcomm® Snapdragon Wear™ platforms are made to deliver low-power, high-impact performance for a wide range of wearables, including smartwatches, kids' watches, smart trackers and more. *
Disabling Lock **Locking Industry**	Qualcomm Technologies announced SafeSwitch in September of 2014. SafeSwitch is available to customers through its Qualcomm Snapdragon 810 processors. SafeSwitch technology - addresses mobile security threat with a kill switch solution is designed to allow device owners to remotely disable their devices in the event that they're lost or stolen - and then re-enable them in the event they're found. This helps to protect sensitive, valuable personal data and to deter device theft. *
Biometrics **Biometrics Industry**	Authenticating the user and the device. Beyond secure fingerprint identification, a Snapdragon 835 Mobile Platform provides a user with an extra level of safety using Camera Security—a camera-based biometric solution for iris and facial recognition engineered to help enhance mobile device security. *

Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
Biometrics **Biometrics Industry**	Mobile transactions are safest when they are protected by a combination of user and device authentication methods. This helps data remain secure from the moment a user logs into their device. A Snapdragon 835 Mobile Platform contains the Qualcomm Haven™ security platform—a combination of hardware, software and biometrics technologies that help to make online banking and payments more secure than ever. *
Cellular and Wireless Modem: Smartwatches **Electronic Device Industry**	Qualcomm supplied the LTE modem in the Apple Watch Series 3. TechInsights found the Qualcomm MDM9635M, a Snapdragon X7 LTE modem in the 42mm sport band model A1861 with GPS + cellular it opened up. The modem was mated in a package-on-package with a Samsung K4P1G324EH DRAM in the watch. Among other wireless chips, TechInsights said the watch contains a Qualcomm PMD9645 PMIC and a WTR3925 RF transceiver. Apple and Qualcomm are embroiled in a handful of patent infringement disputes including investigations at the U.S. ITC, particularly around baseband modems. Apple continues to use the Qualcomm parts in watches despite threats of injunctions. Apple decided to discontinue paying Qualcomm royalties while court cases are in progress.
Cellular and Wireless Modem: Smartphone **Mobile Device Industry**	The iPhone X A1865 uses the Qualcomm MDM9655 Snapdragon X16 LTE modem. iPhone 8; Qualcomm Modem Model A1663; plus 802.11ac Wi Fi with MIMO; Bluetooth 5.0 wireless technology; NFC with reader mode. iPhone 8 Plus; Qualcomm Modem Model A1664; plus 802.11ac Wi Fi with MIMO; Bluetooth 5.0 wireless technology; NFC with reader mode. iPhone 7; Qualcomm Modem Model A1660; plus 802.11ac Wi Fi with MIMO; Bluetooth 4.2 wireless technology; NFC with reader mode. iPhone 7 Plus; Qualcomm Modem Model A1661; plus 802.11ac Wi Fi with MIMO; Bluetooth 4.2 wireless technology; NFC with reader mode. The Qualcomm MDM9625M is a modem LTE chipset found in the Apple MG9M2CL/A iPhone 6 Plus and iPhone 6.
Wi-Fi **Wireless Networking Technology Industry**	With all the devices connecting to all the things, we knew we had to help ease overload. So, we were the first to announce end-to-end commercial support for the next-generation of Wi-Fi. What does that mean? It translates into faster delivery and longer battery life for Wi-Fi devices (e.g., phones)—whether you're at home or on the go. *

Qualcomm's Technological Capability and Industry	Qualcomm's Technological Capability (Description)
Modems **Wireless Networking Technology Industry**	Qualcomm quote: "Some say the modem is the most important part of your smartphone. We couldn't agree more. With our wireless modem inside your smartphone, you've got years of engineering keeping you connected to your great big world. And isn't that why you bought that device in the first place?" *
LTE **Wireless Networking Technology Industry**	Everyone promises smarter/better/faster, but with LTE, we actually delivered. We invented the wireless standards and fundamental technologies that mobile operators rely on to meet the explosive demand in mobile data traffic. And that means you can catch up on the latest sports clips without waiting for the network to keep pace. *
Qualcomm Snapdragon Processor: Smartwatches **Industry for Processors** **Electronic Device Industry**	Samsung Gear S2 3G Watch (Qualcomm Snapdragon 400 Processor); Samsung Gear S Watch (Qualcomm Snapdragon 400 Processor); LG Watch Sport (Qualcomm Snapdragon Wear 2100 Processor); LG Watch Style (Qualcomm Snapdragon Wear 2100 Processor); LG G Watch R (Qualcomm Snapdragon 400 Processor); LG Watch Urban (Qualcomm Snapdragon 400 Processor).
Qualcomm Snapdragon Processor: Smartphone **Industry for Processors** **Mobile Device Industry**	Samsung Galaxy S8 (Qualcomm Snapdragon 835 Processor); Samsung Galaxy Note 8 (Qualcomm Snapdragon 835 Processor); Samsung Galaxy S7 (Qualcomm Snapdragon 820 Processor); Samsung Galaxy S5 (Qualcomm Snapdragon 801 Processor); Samsung Galaxy S4 (Qualcomm Snapdragon 600 Processor); LG V30 (Qualcomm Snapdragon 835 Processor); LG G5 (Qualcomm Snapdragon 820 Processor); LG G4 (Qualcomm Snapdragon 808 Processor); LG G3 (Qualcomm Snapdragon 801 Processor); LG Pro 2 (Qualcomm Snapdragon 800 Processor).
GPS / Navigation **Automobile Industry**	Every time you navigate you've got the power of Qualcomm technology to thank. All the advancements coming to your phone, car, home and community are made possible by the mobile hardware, software and standards we pioneered. Qualcomm invented many of the technologies that the world's leading networks and devices run on. *

- Reference: Qualcomm's Website

CLAIM 1 OF PLAINTIFF'S '497 PATENT

Plaintiff has demonstrated and complied with Patent Local Rule 4 (c) & (d), by specifically pointing out the alleged infringing products' central processing units (CPUs) i.e., chipsets or system-on-a-chip (SoC)s; and, the alleged infringing products' fingerprint biometric lock disablers i.e., lock disabling systems, that Plaintiff believes the Defendant and third-party contractors are infringing Plaintiff's claim limitations under the "doctrine of equivalents". ("substantially the same function in substantially the same way to obtain the same result", quoting *Winans v. Denmead*, 15 How. 330, 344 (1854)) Retrieved from the Opinion filed on 07/29/21, (Dkt. No. 239):

> II. Plaintiff's Contentions Do Not Identify A Locking Feature. Each of the asserted patents ('497, '752, '189, '439, and '287) also require a locking mechanism that is not identified in the accused products. 8 For instance, claim 1 of plaintiff's '497 patent requires: *"detection of specific chemical, biological, or radiological agents or compounds by the detectors causes* the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to *the automatic/mechanical lock disabler to lock or disable the lock of the product* thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals."

Each of Plaintiff's asserted patents ('497, '752, '189, '439, & '287) specifications describes at length various forms of "locking mechanisms". There's no requirement that a locking mechanism is claimed when writing the patents claims.

The only claim limitation the Defendant identified, that they believe is in violation of Patent Local Rule 4(d), is claim 1 of Plaintiff's '497 patent: *"detection of specific chemical, biological, or radiological agents or compounds by the detectors causes… the automatic/mechanical lock disabler to lock or disable the lock of the product… "*

When considering the above segments taken from claim 1 of the '497 patent, Plaintiff has satisfied the requirement of Patent Local Rule 4(c) of "identifying where each element of each asserted claim is found within each accused product, process, or method…" when Plaintiff

specifically identified the chipsets / CPUs of the accused devices, and the biometric fingerprint scanner of the accused devices.

Patent Specifications: "[t]he detection of the particular agent or compound can be conveyed from the detectors to the detector case ***cpu***… [a] ***cpu*** 40 is mounted within the detector case 12 and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment… [t]he detectors 46 are interconnected to the ***cpu*** 40 of the detection system 10 by conventional connections that can be wire or wireless for transmitting the appropriate signals to the ***cpu*** 40 upon detection of the particular agent or compound… [e]ach detector 46 includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the ***cpu*** 40 of the detector case 12… FIGS. 4 and 5 and connected by wire 58 to the ***cpu*** 40 of the detector case 12… [t]he fingerprint biometric lock with disabler 62 is interconnected to the ***cpu*** 40… resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the ***cpu*** 40, then the individual can reset the fingerprint biometric lock with disabler… he lock disabler 56 would be activated upon detection of the harmful agent or compound and receipt of a signal from the ***cpu*** 40… a representative schematic 74 for describing the signal transmission process from the detector 46 to the ***cpu*** 40… detection of the specific agent will trigger the sound alarm 80 and the light alarm 82, and instant transmittal of a signal to the ***cpu*** 40… [t]he readings 84 can be stored by the ***cpu*** 40 for verification and future review and evaluation… the system 10--the ***cpu*** 40--will transmit a lock/disable lock signal 94 to the automatic/mechanical lock disabler 56 to lock or disable the lock on the product… [u]pon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the ***cpu*** 40 would then transmit a signal to the fingerprint biometric lock with disabler 62 to lock or disable the lock on the product… [t]he ***cpu*** 40 would transmit a lock/disable signal 120…"

Patent Specifications: "FIG. 1 is a perspective view of the… an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler… FIG. 14 is a representative schematic view of the… lock disabling system of the present invention illustrating interconnection of the… fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public…

The fingerprint biometric lock with disabler 62 is interconnected to the cpu 40… for receiving transmissions therefrom after detection… has occurred so that the lock… can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler 62 occurs when the fingerprint of the individual is placed on the fingerprint-matching pad 64, and if a match occurs with a known fingerprint stored by the cpu 40, then the individual can reset the fingerprint biometric lock with disabler 56… a fingerprint that matches stored and authorized fingerprints 102 would indicate an authorized individual, and would allow the individual to disable and disarm 104 the lock… The fingerprint biometric lock with disabler 62 would then be reset 106 after the appropriate safety… and protection measures are completed, and the system 10 would be reset and placed back in the detection mode 108"

Example: Security feature: After several unsuccessful log-in attempts using a passcode or fingerprint, an Android device automatically locks itself up. If unable to log in after the security layers, the only option is to have the device unlocked. The wrong pin will launch to Google Account Login. On Android Phone, multiple attempts (usually five attempts) with an unknown or a wrong pin will go either into a 30 seconds delay before further attempts are allowed or the phone will allow entry using your Google account password to unlock the phone. You can have your irises and multiple fingerprints registered along with a backup PIN, pattern or password. "Lock Network & Security" feature as my security net if my phone is stolen. The "Lock Network & Security" feature is supposed to prevent anyone else from turning OFF your phone and your wifi/data when your phone is locked, for purposes such guaranteeing that you will still be able to track or remotely control your phone when it is lost or stolen.

Therefore, when a signal is received at the CPU, signifying a security threat (unauthorized user, detection of a bomb, lost or stolen device), the CPU processes instructions to lock or disable the lock on the Defendants' accused devices.

Plaintiff has demonstrated and complied with Patent Local Rule 4 (c) & (d), by specifically pointing out the alleged infringing products' central processing units (CPUs) i.e., chipsets or system-on-a-chip (SoC)s; and, the alleged infringing products' fingerprint biometric lock disablers i.e., lock disabling systems, that Plaintiff believes the Defendant and third-party contractors are infringing Plaintiff's claim limitations under the "doctrine of equivalents". ("substantially the same function in substantially the same way to obtain the same result", quoting *Winans v. Denmead*, 15 How. 330, 344 (1854))

Even if there is no literal infringement, a claim may be infringed under the doctrine of equivalents if some other element of the accused device or process performs substantially the same function, in substantially the same way, to achieve substantially the same result. The "doctrine of equivalents" is a judicially created doctrine having three parts "function/way/result" substantial identity test.

The Defendant challenged only one (claim 1 of the '439 patent) of the twenty-five patent claims asserted in this case. Even if the Court found that claim 1 of the '439 patent is not infringed by the third-party contractors, that does not automatically cause the dismissal of the remaining twenty-four patent claims of the '752, '189, '439, & '287 patents, asserted in this case.

The Defendant (United States) must show non-infringement of each of the remaining twenty-four patent claims of the '752, '189, '439, & '287 patents asserted in this case. The Defendant need only infringe one valid patent claim to be liable for infringement.

This Court has the authority to cancel, invalidate, and even dismiss Plaintiff's claim 1 of the '439 patent, if the Court determines Plaintiff has not complied with the requirement of Patent Local Rule 4(c). This Court also has the authority to grant Plaintiff relief to all, or any one of, the remaining twenty-four patent claims of the '752, '189, '439, & '287 patents.

It is improper and scandalous for the Defendant to ask for a dismissal of Plaintiff's entire case base on the Defendant's belief that claim 1 of the '439 patent does not infringe, or that Plaintiff has not given the Defendant notice regarding the *"detection of specific chemical, biological, or radiological agents or compounds by the detectors causes… the automatic/mechanical lock disabler to lock or disable the lock of the product… "*

DEFENDANT'S INVALIDITY CONTENTIONS

Defendant submitted its Notice to the Court in Case 1:13-cv-00307-EGB; Document 238; Filed 07/08/21: "Defendant the United States (the Government) hereby provides notice that on Friday, June 25, 2021, the Government served its Preliminary Disclosure of Invalidity Contentions on Plaintiff, pursuant to the Court's March 29, 2021 Scheduling Order (Dkt. 221) and PRCFC 6." The Defendant asserted the patent references of Breed, Benson, Webb, Garabedian, Astrin, and Mostov.

The Breed reference is the only reference that antedates the conception date established under Patent Local Rule 4(e) by Plaintiff of December 16, 2002. The Breed reference nullifies and renders redundant the other refences of Benson, Webb, Garabedian, Astrin, and Mostov because the Breed reference under 102-anticipation because Breed has the earlier priority date. See the chart below.

> "[a]nticipation under 35 U.S.C. § 102 requires the presence in a single prior art disclosure of each and every element of a claimed invention.… [t]hat which would literally infringe if later in time anticipates if earlier than the date of invention."

Breed does not qualify as a valid prior art reference to Plaintiff's asserted patents-in-suit ('497, '752, '189, '439, & '287) for the following reasons:

- The Breed reference was asserted against the Plaintiff in an IPR trial. "IPR estoppel applies to "any ground that the petitioner raised or reasonably could have raised during that *inter partes review*." 35 U.S.C. § 315(e). As recently as 2018, there was uncertainty about the scope of *inter partes review* (IPR) estoppel under 35 U.S.C. § 315(e)(2). Under a broad interpretation, IPR estoppel precludes petitioners from asserting in a district court any grounds raised or that could have been raised in their IPR petitions."
- During the 18 months of the IPR trial, the Plaintiff sent the Breed reference over to the USPTO for prosecution of the nine (9) patent claims asserted in this case, of the now issued '189 patent. The USPTO stated the Breed reference does not cover the Plaintiff's patent claims as a hold. Plaintiff submitted as "information disclosure statements", the Breed reference to the USPTO for prosecution of the eleven (11) patent claims asserted in this case of the now issued '439 patent, and the prosecution of the three (3) patent claims asserted in this case of the now issued '287 patent.
- Submitting the Breed reference violates Patent Local Rule 7(b). "PATENT RULES OF THE UNITED STATES COURT OF FEDERAL CLAIMS: Rule 7. Document Production Accompanying Preliminary Disclosure of Invalidity Contentions. Together with the Preliminary Disclosure of Invalidity Contentions, the defendant and any defendant-intervenors must produce to each opposing party, or make available for inspection or copying: (b) a copy of any additional items of prior art identified that do not appear in the file history of each patent at issue."

- Plaintiff's patents are presumed valid. "[w]ith *Microsoft v. i4i*, the Supreme Court confirmed the status quo, that the clear-and-convincing standard is the single standard for proving patent invalidity. The Court acknowledged, however, that the burden of proof may be easier to meet when evidence touching the validity of the patent was not considered by the PTO… Much of the uncertainty leading up to the i4i decision derived from language in the Supreme Court's recent decision in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007) ("KSR"). KSR stated that, when evidence before the fact finder was not before the PTO during procurement, "the rationale underlying the presumption-that the PTO, in its expertise, has approved the claim-seems much diminished." *In i4i*, the Supreme Court harmonized KSR with its conclusion that the statute requires a clear-and-convincing standard of proof of invalidity. New evidence supporting an invalidity defense may 'carry more weight' before the fact finder than evidence previously considered by the PTO." As articulated by Judge Rich in *American Hoist & Derrick Co. v. Sowa & Sons, Inc.*, 725 F.2d 1350 (Fed. Cir. 1984):

  > When new evidence touching validity of the patent not considered by the PTO is relied on, the tribunal considering it is not faced with having to disagree with the PTO or with deferring to its judgment or with taking its expertise into account. The evidence may, therefore, carry more weight and go further toward sustaining the attacker's unchanging burden.

Order of Priority	Asserted References
1ST	Breed, Appl. No.: 11/946,928, filed on Nov. 29, 2007, Pub. No.: US 2008/0094212 A1, Pub. Date.: April 24, 2008, Provisional application No. 60/387,792, filed on ***Jun. 11, 2002***.
2ND	Webb, Appl. No.: 10/464,523, filed on ***June 17, 2003***, Pub. No.: US 2004/025722 A1, Pub. Date.: Dec. 23, 2004, No Provisional application filed.
3RD	Mostov, Appl. No.: 11/343,560, filed on Jan. 30, 2006, Pub. No.: US 2006/0181413 A1, Pub. Date.: Aug. 17, 2006, Provisional application No. 60/648,260, filed on ***Jan. 28, 2005***.
4TH	Garabedian, Appl. No.: 11/065,865, filed on ***Feb. 25, 2005***, Pub. No.: US 2006/0191324 A1, Pub. Date.: Aug. 31, 2006, No Provisional application filed.

5TH	Benson, Appl. No.: 11/418,380, filed on May 3, 2006, Pub. No.: US 2007/OO3O143 A1, Pub. Date.: Feb. 8, 2007, Provisional application No. 60/677,164, filed on ***May 3, 2005***.
6TH	Astrin, Appl. No.: 11/414,479, filed on April 28, 2006, Pub. No.: US 2006/0250235 A1, Pub. Date.: Nov. 9, 2006, Provisional application No. 60/678,454, filed on ***May 4, 2005***.

THE PRELIMINARY INFRINGEMENT CONTENTIONS GIVES NOTICE TO HOW THE GOVERNMENT HAS TAKEN FOR THE BENEFIT OF THE PUBLIC, PLAINTIFF'S CLAIMED INVENTIONS; AND, CAUSE THE MANUFACTURE AND "UBIQUITOUS" COMMERCIALIZATION OF PLAINTIFF'S CLAIMED INVENTIONS

"Ubiquitous" in the U.S. Department of Homeland Security, 2007 Cell-All Ubiquitous Biological and Chemical Sensing Solicitation, is defined as: "present, appearing, or found everywhere"; "existing or being everywhere at the same time"; "ubiquitous is something that seems to be present at the same time, everywhere"

> Mobile phones are ubiquitous today. The portable device has revolutionized the way we communicate with one another locally and globally. They have enabled the populace to be connected to one another in case of a crisis even from a remote area. Today real-time communication is possible at any time and from any part of the globe. Cell phones have become a necessity in today's digital global society, and are not just a symbol of social status anymore. In developing countries, they are being considered as the fifth necessity in addition to food, clothes, shelter, and education. (BusinessWeek Online Extra ,2007)
>
> Who doesn't own a Smartphone? Right from teenagers to senior citizens and from businesspersons to business leaders, Smartphone ownership is Ubiquitous and all pervasive. Indeed, it is estimated that nearly 80% of the world's population is now connected to each other through the mobile phones with Smartphones constituting the majority of such devices. From the time the Late Legendary Steve Jobs unveiled the iPhone and set off a revolution in the way we live and work, the Smartphone has been on an unstoppable journey towards transforming business and commerce. (Article Written By "Prachi Juneja" and Reviewed by Management Study Guide Content Team)

Research contracts were awarded by DHS through HSARPA and the Small Business Innovation Research Portfolio, with some of the primary recipients being Qualcomm, Synkera Technologies, and NASA (U.S. Department of Homeland Security, 2011b). In addition, DHS

S&T secured Cooperative Research and Development Agreements with four primary cell phone manufacturers—Qualcomm, LG, Apple, and Samsung—with the objective of accelerating the ‘‘commercialization of technology developed for government purposes’’ (U.S. Department of Homeland Security, 2010). **(Qualcomm—Exhibits A & B)**

As a personal sensing and alerting system, Cell-All promises to protect a diverse and inclusive range of individuals, from ‘‘a grandmother taking a siesta [to] a teenager hiking through the woods...’’ (U.S. Department of Homeland Security, 2010)

As DHS’s Stephen Dennis explained, ‘‘We didn’t just do the science work here; we actually did look at the market’’ (Dennis, 2011). With Qualcomm’s help, DHS assessed commercial viability through market research, asking what conditions would need to be met for the public to both accept and pay for the system. Based on this market research, DHS concluded:

> What we learned is that the personal protection application will sell the device. People will actually turn in their [current] phone, get a new phone, if it provides them with a magnitude of personal protection, especially for families, people with aging parents, people with young children. (Dennis, 2011)

> When we asked our nation’s first responders to name the deadliest gas for us, in terms of what the American population faces as a threat, carbon monoxide was it...it actually establishes a basis for commercial manifestation of what we’ve done here. (Dennis, 2011)

The Cell-All program is funded and managed by HSARPA, whose mission is to facilitate the rapid development and deployment of new security technologies, mainly through partnerships and contracts with the private sector (U.S. Department of Homeland Security, 2011a). As DHS representatives explain it:

> The most important component of all is delivering the technology into the hands of those who need it so that we’re not one of those government R&D labs that’s happy to throw something over the wall or end it with a paper. We’re actually trying to take this technology all the way to the end. (Dennis, 2011)

> We believe that technology transfer directly to the commercial [sector] is an efficient way to go. We know that there are a number of commercial opportunities that have been provided to our sensor manufacturers and to the folks who are involved in this program, so we’re looking forward to taking advantage of those [opportunities] directly. (Dennis, 2011)

HSARPA accelerates this process through direct commercial partnerships, where it funds researchers from both the public and the private sector to develop products that can then be brought to market, even if the only buyers are government agencies. From the start, though, the

program has fostered public–private partnerships under the assumption that government agencies are too slow or lack the expertise to develop such a system on their own. This position is neatly articulated by HSARPA:

> The acceleration of integrated environmental sensing and the utilization of mobile computing platforms for homeland security establishes a leading-edge capability instead of a traditional trailing edge capability that government sometimes has, taking advantage of the latest in new chemical sensor innovation. Delivering these capabilities to the extended homeland security enterprise as a commercial capability makes government technology transfer easier and far more efficient than trying to nurse it along inside of government, so I'm very excited that we have commercial opportunities to take advantage of the technology that's been created here. (Dennis, 2011)

Enrolling members of the public could be seen as an entrepreneurial move on the part of DHS to exploit existing public resources, in the form of people with smartphones, to meet its narrowly defined public-safety objectives; as a Qualcomm representative argued: ''Let's take advantage of the 300 million cell phones that are out there today. They're always with us'' (Hoffman, 2011). Widespread participation is needed, with members of the public serving as passive data-collection nodes.

Qualcomm's role has been to develop a smartphone app and the associated network software for processing data. Smartphone users can download the app from Google Play and, eventually, from Apple's iTunes store, so Cell-All will be operational on all phones using either Google's Android or Apple's iPhone operating systems. When the application is installed, it will ask the user for permission to share sensor readings and location information over the network; then, whenever abnormal chemical levels are detected, the phone will send those data to a network gateway. According to Doug Hoffman, program manager at Qualcomm…

This orientation is evinced by Cell-All's early-stage market research, paid for by HSARPA and administered by Qualcomm **(Qualcomm—Exhibits A & B)**. After finding a viable market, industry partners were further persuaded by government contracts to develop systems and services and by the high probability of sustained profits from a range of customers after product development. Clearly, having privileged access to consumer data, even in de-identified, aggregate form, would be of great interest to partnering companies.

CONCLUSION

"[A] party need not identify every piece of evidence on which it will ultimately rely to show infringement in its infringement contentions. Instead, it need only identify 'where each element of each asserted claim is found within each Accused Instrumentality." *In re Innovation IP Ventures, LLC Patent Litig.*, 956 F. Supp. 2d 925, 940-41 (N.D. Ill. 2013) (Holderman, C.J.).

The Defendant is trying to convince this Court that Plaintiff's central processing units (CPUs) are insignificant to these proceedings, but has introduced Benson's, (Patent No. 7,656,286 B2), "TRUSTED MONITORING SYSTEM AND METHOD", microprocessors as prior art to challenge Plaintiff's asserted patents' central processing units (CPUs).

Benson's '286 filing date does not antedate Plaintiff's '497 filing; does not antedate Plaintiff's Disclosure with the PTO on 11/26/04; or, Plaintiff's date of conception of 12/16/02.

Benson does not disclose a microprocessor connection for radio-frequency near-field communication; a disabling locking mechanism; chemical or biological detection; a fingerprint biometric lock disabler after multiple failed attempts to open; a communication device of at least a cell phone or smartphone; or, an internet or wi-fi connection. Benson's claimed invention is anticipated by Plaintiff's claimed inventions.

Plaintiff contends that the Defendant's Motion should be stricken, because the motion contain one or more of the following defects: irrelevant and useless matter; immaterial and unimportant matter; impertinent, inappropriate, and out of place matter), redundant matter that is no longer needed or useful; and scandalous outrageous untruthful matter.

Allowing the Motion to remain in the record would be detrimental, damaging, harmful, and hurtful to the Plaintiff because it forces the Plaintiff to respond to issues that are no longer needed or useful, and to respond to things that are unnecessary or could be left out.

Therefore, Plaintiff is seeking "Summary Judgement" in favor of the Plaintiff, because the Defendant's Motion is overly broad, unduly burdensome and is not reasonably calculated to lead to the discovery of evidence not already submitted into the record. Plaintiff believes the Defendant has exhausted all measures and has reduced his defense down to a "copy and paste" procedural violation.

Qualcomm, Apple, Samsung, and LG, has refused to appear. The Government continuing to defend the third-party multi-billion-dollar corporations, when they decline to defend themselves, is evidence there's nothing left to litigate. Summary Judgement in the Plaintiff's favor is appropriate.

References

BusinessWeek Online Extra. (24 September, 2007). India's Cell-Phone Ride Out of Poverty. Retrieved from http://www.businessweek.com/magazine/content/07_39/b4051058.htm

Dennis, S., (2011). Cell-All Program Overview. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. (Accessed 17.09.12).

Hoffman, D., 2011. Qualcomm Project Presentation. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. (Accessed 17.09.12)

Juneja, P. (2015). The Ubiquitous Smartphone and how it has Transformed Business and Commerce. https://www.managementstudyguide.com/ubiquitous-smartphone-and-how-it-has-transformed-business-and-commerce.htm

U.S. Department of Homeland Security, 2007. Cell-All Ubiquitous Biological and Chemical Sensing. (Accessed 17.09.12).

U.S. Department of Homeland Security, 2010. Cell-All: Super Smartphones Sniff Out Suspicious Substances. (Accessed 17.09.12).

U.S. Department of Homeland Security, 2011a. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. (Accessed 17.09.12).

U.S. Department of Homeland Security, 2011b. Privacy Impact Assessment for the Cell All Demonstration. (Accessed 19.09.12).

U.S. Department of Homeland Security, 2011c. Transcript of the Meeting of the Data Privacy and Integrity Advisory Committee. May 19. (Accessed 17.09.12).

Respectfully submitted,

s/ Larry Golden

Larry Golden, Plaintiff, Pro Se

740 Woodruff Rd., #1102

Greenville, South Carolina 29607

atpg-tech@charter.net

864-288-5605

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 7th day of September, 2021, a true and correct copy of the foregoing "Plaintiff's Response to Defendant's Motion to Strike and Plaintiff's Motion for Summary Judgement", was served upon the following Defendant via e-mail:

Grant D. Johnson
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
Grant.D.Johnson@usdoj.gov
202-305-2513

s/ Larry Golden
Larry Golden, Pro Se
740 Woodruff Rd., #1102
Greenville, South Carolina 29607
atpg-tech@charter.net
864-288-5605